
ICE Data Services Limited Acceptable Use Policy

© 2014 Intercontinental Exchange Group. All rights reserved. No part of this material may be copied, photocopied or duplicated in any form by any means or redistributed without the prior written consent of Intercontinental Exchange. All third party trademarks are owned by their respective owners. The Intercontinental Exchange and its affiliates do not recommend or make any representation as to possible benefits from any securities or investments, or third-party products or services. Investors should undertake their own due diligence regarding securities and investment practices. This material may contain forward-looking statements regarding Intercontinental Exchange and its affiliates that are based on the current beliefs and expectations of management, are subject to significant risks and uncertainties, and which may differ from actual results. All data as of 1 April 2014. The Intercontinental Exchange disclaims any duty to update this information.

Exhibit A

Acceptable Use Policy

INTRODUCTION

This Acceptable Use Policy (the "Policy") defines acceptable practices for the use of ICE Data Services Limited ("ICE Data Services") services (the "Service(s)"). The Policy applies to all aspects of the Service. "ICE Data Services" means ICE Data Services Limited and all of its affiliates (including direct and indirect subsidiaries and parents).

By using the Services, any such user of the Services (the "Customer") is responsible for compliance with this Policy. The Customer is responsible for violations of this Policy by any person or entity that accesses the Services through the Customer's agreement with ICE Data Services or through the Customer's equipment, systems, networks, or other facilities ("Affiliated Person(s)"). Any Affiliated Person using the Services is bound, as specified in this Policy, by the same acceptable practices as the Customer. Whilst ICE Data Services is not obligated to control or monitor the online experience or the content of online communications in connection with the Service, ICE Data Services may edit or remove content that it deems to be in violation of any applicable law or regulation, or either the letter or spirit of this Policy, or that it otherwise deems unlawful, harmful or offensive.

This Policy is designed to assist in protecting ICE Data Services, the Services, Customers and the online community as a whole from improper and/or illegal activity over or utilising the Service, the Internet, and other systems and networks. In situations where data communications are carried across networks of other service providers or via third party application service providers (together, the "Providers"), the Customer must also conform to the applicable acceptable use policies of the Providers.

Rights of ICE Data Services

SUSPENSION OR TERMINATION OF SERVICE

If, in ICE Data Services' reasonable judgment, the Customer engages in conduct whilst using the Service that violates this Policy, ICE Data Services reserves the right to suspend and/or terminate the Service or any part thereof. ICE Data Services will generally attempt to notify the Customer of any activity in violation of the Policy and request that the Customer cease such activity; however, in cases where ICE Data Services' services or its software, programs, products, networks, systems, business or business reputation is threatened, including without limitation cases involving unsolicited commercial email/SPAM, mail relaying, invasive and unauthorised data gathering/mining, alteration of the Customer source IP address information, denial of service attacks, noncompliance with applicable laws and regulations, suspected fraud in connection with the use of the Service, the dissemination of viruses, "Trojan horses", and spyware, offensive material or copyright infringement, order of a court or regulatory authority of competent jurisdiction, threat of imminent harm to persons or property or any other act ICE Data Services deems, in its sole discretion, to be in violation of this Policy, ICE Data Services reserves the right to suspend or terminate the Service without notification to the Customer. In addition, ICE Data Services may take any other appropriate action against the Customer for violations of this Policy. This Policy extends to any and all content created by the Customer, including but not limited to discussion boards, blogs, wikis, social networking sites, news sites, mobile photos and videos, customer review sites, experience or photo sharing sites, any other website or forum that offers the opportunity

for the consumer to share their knowledge and familiarity with a product or experience that Customer uses during the term of any Service ("User-Generated Content"). ICE Data Services does not have any obligation to monitor or police activity occurring in connection with the Service and will not be liable to any party, for any violation of this Policy.

NO RESPONSIBILITY

ICE Data Services shall have no responsibility for any information or material created, stored, maintained, transmitted by the Customer or otherwise accessible through using or in connection with the Service.

RESERVATION OF RIGHTS

Nothing in this Policy shall limit in anyway ICE Data Services' rights and remedies at law or in equity that may otherwise be available.

COOPERATION WITH INVESTIGATIONS

ICE Data Services will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity. ICE Data Services reserves the right to disclose Customer information to the extent authorised by applicable law.

COMPLAINTS

ICE Data Services receives complaints directly from Internet users, through Internet organisations and through other parties. ICE Data Services shall not be required to determine the validity of complaints received before taking action under this Policy. ICE Data Services, in its sole discretion, reserves the right to forward these complaints to the appropriate law enforcement agencies.

MODIFICATIONS TO POLICY

ICE Data Services reserves the right to modify this Policy at any time without notice. ICE Data Services will attempt to notify the Customer of any such modifications either via e-mail or by posting a revised version of the Policy on the ICE Data Services website, but the Policy will be in effect when posted unless otherwise stated and the Customer will be bound thereby whether or not they have received notice.

FILTERS AND OTHER SECURITY MEASURES

ICE Data Services reserves the right to install and use, or to have the Customer install and use in connection with the Customer's equipment, systems, and networks, any appropriate measures, including without limitation devices, hardware, software, practices, protocols and/or techniques to prevent violations of this Policy, including but not limited to, monitoring, scanning, vulnerability testing and installing devices designed to filter or terminate access to the Service.

Prohibited Uses

ILLEGAL ACTIVITY

The Service shall not be used for any unlawful activities or in connection with any criminal or civil violation and the Service shall in all cases be used in compliance with applicable law and regulation. Use of the Service in any manner, including without limitation for transmission, distribution, retrieval, or storage of any information, data or other material, in violation of any applicable law or regulation (including, where applicable, any tariff or treaty) is prohibited.

OFFENSIVE MATERIALS

The Customer shall not disseminate or post material in any forum, online or otherwise, that is improper, including without limitation material that is unlawful, libellous, defamatory, obscene, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory or otherwise objectionable. This includes Customers as a content creator for third parties. Without limiting the foregoing, the Customer shall not access or use the Service in any manner for the transmission or dissemination of images containing child pornography. Offensive Materials extend to any and all User-Generated Content that the Customer uses during the term of any Service.

INFRINGEMENT

The Customer shall not use or transmit any data or material protected by copyright, service mark, trademark, trade secret, patent or other intellectual property right without proper authorisation.

EXPORT VIOLATIONS

The Customer shall not violate any applicable export control laws and regulations.

UNAUTHORISED ACCESS/INTERFERENCE

The Customer shall not attempt to gain unauthorised access to, or attempt to interfere with or compromise the normal functioning, operation or security of the ICE Data Services network or other systems or networks. The Customer shall not use the Service to engage in any activities that may interfere with the ability of others to access or use the Service or the Internet. The Customer shall not use the Service to monitor, gather or mine any data, information or communications on any network or system without authorisation. The Customer shall not attempt to gain unauthorised access to the user accounts or passwords of other Customers.

UNSOLICITED COMMERCIAL EMAIL/SPAMMING/MAILBOMBING

The Customer shall not use the Service to transmit unsolicited commercial e-mail messages or deliberately send excessively large attachments to one recipient. Any unsolicited commercial e-mail messages or a series of unsolicited commercial e-mail messages or large attachments sent to one recipient is prohibited. In addition, "spamming" or "mail bombing" is prohibited. Use of the service of another provider to send unsolicited commercial email, spam or mail bombs, to promote a site hosted on or connected to the Service or any of ICE Data Services' equipment, systems, networks, or other facilities, is similarly prohibited. Likewise, the Customer shall not use the Service to collect responses from mass unsolicited e-mail messages. A complaint from the recipient of commercial email, whether

received directly or through an anti-spamming organisation, shall be evidence that the message was unsolicited. ICE Data Services has no obligation to forward the complaint to the Customer or to identify the complaining parties.

SPOOFING/FRAUD

The Customer is prohibited from intentionally or negligently injecting false data into any network, including but not limited to bad routing information (the announcing of networks owned by someone else or reserved by the Internet Assigned Numbers Authority) or incorrect DNS information.

The Customer shall not send, or attempt to send e-mail messages or transmit any electronic communications using a name or address of someone other than such Customer. Any attempt to impersonate someone else by altering source IP address information or by using forged headers or other identifying information is prohibited. Any attempt to fraudulently conceal, deceive, forge or otherwise falsify the Customer's identity in connection with use of the Service is prohibited.

USENET POSTINGS

All postings to USENET groups shall comply with that group's charter and other policies. Users are prohibited from cross posting to unrelated news groups or to any news groups where the post does not meet that group's charter. Continued posting of off-topic messages, including commercial messages (unless specifically invited) is prohibited. Disrupting newsgroups with materials, postings or activities that are (as determined by ICE Data Services in its sole discretion) frivolous, unlawful, libellous, defamatory, obscene, indecent, lewd, harassing, threatening, harmful, invasive of privacy and publicity rights, abusive, inflammatory, or otherwise objectionable, including being excessive or repetitious, unless such materials or activities are expressly allowed or encouraged under the newsgroup's name, FAQ or charter, is likewise prohibited.

FAILURE TO ABIDE BY THIRD-PARTY PROVIDER POLICIES

The Customer shall not violate the rules, regulations, or policies that apply to any Providers, network, server, computer database, or website that the Customer accesses.

CUSTOMER COLOCATION AT THE EUROPEAN LIQUIDITY CENTER

Any Customer utilising Services at ICE Data Services' European Liquidity Centre at Basildon may utilise such Services solely for trading purposes and not for the routing, hosting or transmission of any data and/or content over, by or through the Internet unless via an ICE Data Services sponsored VPN.

OTHER PROHIBITED ACTIVITIES

The following activities, without limitation, are also prohibited:

- I. Any attempt to circumvent, alter or reverse engineer any processes, procedures, protocols, algorithms and or applications utilised in the provision of or use of the Services.
- II. Any attempted transmission of files containing a computer virus or corrupted data.
- III. Any advertising, transmission, distribution, retrieval, storage or otherwise making available any software, program, product, or service that is designed to violate this Policy which includes, without limitation the facilitation of the means to deliver unsolicited commercial email.

- IV. Any use of the Service in excess of any limitations that have been established by ICE Data Services, including, but not limited to specified bandwidth limitations.
- V. Any activity that disrupts, degrades, harms or threatens to harm the Service or ICE Data Services network, or the equipment, services or networks of any other party including, without limitation, viruses, "Trojan horses", worms, time bombs, zombies, cancelbots or any other computer programming routines that may damage, interfere with, intercept or seize any system, program, data or personal information.
- VI. Any use of another party's electronic mail server to relay email without express permission from such other party.
- VII. Any other inappropriate activity or abuse of the Service (as determined by ICE Data Services in its sole discretion), whether or not specifically listed in this Policy, shall result in suspension or termination of the Customer's access to or use of the Service.

This listing of prohibited activities is not exhaustive and ICE Data Services reserves the right to determine that any conduct that is or could be harmful to ICE Data Services, Customers, or Internet users, is in violation of this Policy and to exercise any or all of the remedies contained in this Policy.

Responsibilities of Customers

SECURITY AND CONTENT

The Customer is solely responsible for maintaining the security of its network, software, program, product, services, equipment and applications. The Customer agrees to immediately notify ICE Data Services of any unauthorised use of the Service or any other breach of security known to the Customer. If the Customer becomes aware of any violation of this Policy by any person, the Customer is required to notify ICE Data Services. The Customer shall be solely responsible for any information or material they maintain, transmit, download, view, post, distribute, or otherwise access or make available on, through, using or in connection with the Service.

IMPENDING SECURITY EVENT NOTIFICATION

The Customer is responsible for notifying ICE Data Services immediately if the Customer becomes aware of an impending event that may negatively affect the Services. This includes extortion threats that involve threat of "denial of service" attacks, unauthorised access, or other security events. The Customer shall cooperate with ICE Data Services in investigating, preventing, and/or connecting any actual or apparent breach of this Policy.

CONFIGURATION

The Customer is responsible for configuring its own systems to provide the maximum possible accountability and industry-standard security features. ICE Data Services shall not be liable for any damage caused by such system configurations regardless of whether such configurations have been authorised or requested by ICE Data Services. For example, the Customer should ensure there are clear "path" lines in news headers so that the originator of a post may be identified. The Customer should also configure their Mail Transport Agents (MTA) to authenticate (by look-up on the name or similar procedures) any system that connects to perform a mail exchange, and should generally present header data as clearly possible. As another example, the Customer should maintain logs of dynamically assigned IP addresses.

The Customer is responsible for educating itself with regard to standard financial industry practices for system security. Should systems at the Customer's site be violated, the Customer is responsible for reporting the violation and then fixing the exploited system. For instance, should a site be abused to distribute unlicensed software due to a poorly configured FTP (File Transfer Protocol) server, the Customer is responsible for re-configuring the system to stop the abuse. Irrespective of any items to the contrary in any agreement between the Customer and ICE Data Services, ICE Data Services reserves the right to audit the Customer and to take all appropriate actions to ensure compliance with all requirements of this Policy.

PRIVACY

ICE Data Services makes no guarantee regarding, and assumes no liability for, the security and integrity of any data or information the Customer transmits via the Service or over any network, including any data or information transmitted via any server designated as secure.

GOVERNING LAW

This Policy is governed by and construed in accordance with English law. The courts of England shall have exclusive jurisdiction to hear and settle any action, suit, proceeding or dispute in connection with this Policy notwithstanding the presence of multiple defendants or the introduction of third parties, even for urgent proceedings, appraisals or conservation measures by expedited procedure or by filing a petition.

COMPLAINTS AND CONTACT INFORMATION

In most cases, ICE Data Services will notify the Customer of complaints received by ICE Data Services regarding an alleged violation of this Policy. The Customer agrees to promptly investigate all such complaints and take all necessary actions to remedy any violations of this Policy. ICE Data Services may inform the complainant that the Customer is investigating the complaint and may provide the complainant with the necessary information to contact the Customer directly to resolve the complaint. The Customer shall identify a representative for the purposes of receiving such communications.

Any complaints regarding prohibited use or other abuse of the Services, including violations of this Policy, should be sent to ICE Data Services. Please include all applicable information that will assist ICE Data Services in investigating the complaint, including all applicable headers of forwarded messages.

If the Services are experiencing live attacks, Customers should call into the ICE Data Services Help Desk at +44 (0)20 7488 5100 (ICEHelpdesk@theice.com) to submit a complaint as quickly as possible. Should they need immediate attention, the Customer should describe the urgency of the situation. If the Customer is unsure whether any contemplated use or action is permitted, please submit questions or comments to ICE Data Services.